FSA draft policy vs. ED draft policy

Findings of Interest

Management Controls

- ED does not require an analysis to be performed on the criticality, sensitivity, and integrity of a system's data.
- ED requires risk assessments be performed every five years, rather than every three years in FSA policy.
- ED does not require every system to conduct a mission/business impact analysis prior to implementing findings of the risk assessment.
- ED does not require Self-Assessments. FSA policy requires a self-assessment at least once every three years.
- ED does not require NIST 800-18 compliant security plans. In fact, the only mention of the requirement for a security plan is located in the position description of a Business Manager and Computer Security Officer.
- ED does not require the establishment of rules of behavior to control access to, and the use of, equipment that permits access to agency systems.
- ED does not require the inclusion of security resources in budget requests. Additionally, ED policy does not require the IRB to ensure any investment requests include needed security resources.
- ED policy does not provide recommended security language to be included in contracts or statements of work.
- ED policy does not mention requirements in the solicitation documents to update security controls as new threats/vulnerabilities and as new technologies are implemented.
- ED does not dictate minimum requirements for achieving an interim approval to operate. FSA mandates the completion of a risk assessment, a draft security plan, and project plan for interim accreditation.

Operation Controls

- ED does not require the creation of hiring, transferring, or termination procedures.
- ED does not require a process for requesting, establishing, issuing, and closing user accounts.
- ED does not require a nondisclosure agreement statement if an individual needs access to privileged information.
- ED only requires contract positions, not SFA position, be reviewed for sensitivity level.
- The Department's policy on physical and environmental protection is weak. SFA policy provides substantially more detail.

- ED does not require visitors, contractors, and maintenance personnel to be authentication through the use of preplanned appointments and identification checks. ED policy also does not require the above access group to be escorted when in restricted or sensitive areas.
- ED does not require controls to be in place for transporting or mailing media or printed output.
- ED does not require procedures be established to ensure that unauthorized individuals cannot read, copy alter, or steal printed or electronic information.
- ED does not require the assignment of responsibilities for recovery after a disaster.
- ED does not require the results of the latest be incorporated into the disaster recovery plan.
- ED does not include several critical policies in their DRP/COOP guidance.
- The Department's Virus Detection and Elimination policy is weak. SFA policy directs every system to establish procedures to verify information regarding malicious software, and ensure that incoming warnings are accurate and not a hoax.
- ED does not require a description of intrusion detection tools installed on the system, where they are placed, the type of processes detected/reported, and the procedures for handling instructions.
- ED does require routine review of intrusion detection reports.
- ED does not require new and revised hardware and software to be authorized, tested, approved and documented before distribution and implementation.
- ED does not require the reporting of incidents to FedCIRC, NIPC and local law enforcement when necessary.

Technical Controls

- ED does not provide guidance for users who have the authority/capability to bypass/override system security controls and any compensating controls. FSA policy issues numerous policy statements on the subject, including the requirement to issue a different user ID than the normal business use ID to those users who can bypass security controls.
- ED policy does not provide useful guidance on host-based identification, biometrics, or public key infrastructure.
- ED does not require the maintenance and encryption of a current list of authorized users and their access privileges.
- ED does not indicate how often ACLs should be reviewed to identify and remove users who have left the organization, users whose duties no longer require access to the application, or redundant user IDs and accounts.
- ED does not issue direct agency administrators to create ACLs that restrict users to the level of information to which they are authorized to gain access. FSA policy discusses this area and additionally requires access control lists restrict and control access to all program libraries, system software, and system hardware.

- ED does not require terminals to log-off and screensavers lock after a given period of inactivity.
- ED does not require systems to describe the type of security gateway or firewall in use, including its configuration.
- ED does not issue policy on disabling insecure protocols unless specifically required by the system.
- ED does not require a review of system interconnections, including the unique identifier for each interconnected systems and a description of the interactions among systems.
- ED does not require every web page to have a designated author or maintainer.
- ED does not forbid information protected by the Privacy Act from being posted on publicly accessible web servers.
- ED does not require that log on banners include the notification that it is a government system.
- ED does not require the use of automated tools be used to monitor and assess audit logs.
- ED does not have a policy on keystroke monitoring.
- ED does not identify a policy for the separation of duties between security personnel who administer the access control function and those who administer the audit trail.